UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/761,243	01/22/2004	Yoshihiro Oba	3119-101	2019

52190 7590 07/26/2005

WATCHSTONE P + D
1300 EYE STREET, NW
SUITE 400 EAST
WASHINGTON, DC 20005

EXAMINER	
SHAH, CHIRAG G	

ART UNIT	PAPER NUMBER
2664	

DATE MAILED: 07/26/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/761,243	OBA ET AL.	
	Examiner	Art Unit	
	Chirag G. Shah	2664	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 January 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-60* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12,17-21,24-30,35,38-46 and 52-60* is/are rejected.

7)☒ Claim(s) *13-16,22,23,31-34,36,37 and 47-51* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 January 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-4, 6-8, 17, 24-26, 55-57, and 59 rejected under 35 U.S.C. 102(b) as being anticipated by Agrawal et al (U.S. Pub. 2002/0118656), herein after referred as Agrawal.

Regarding claim 1, Agrawal discloses in **fig. 2A** of a method for seamless hand-off of a mobile device **[mobile station 230, fig. 2A]** between access points **[access points 220-1n, fig. 2A]**, comprising:

pre-configuring a mobile station **[mobile station 230, fig. 2A]** with higher-layer information **[IP address information, paragraph 0025]** for at least one new candidate IP subnetwork **[neighboring cell, fig. 2A and paragraph 0025]**while said mobile station is configured for communications with a present IP subnetwork **[as disclosed in paragraph 0025, a base station serving a mobile station preconfigures the mobile station by sending a list of neighboring candidate cell IP addresses to the mobile station prior to the mobile station entering into a candidate/neighboring cell]** as claim.

Regarding claim 2, Agrawal describes in **fig. 2A** of a seamless handoff from one cell to a neighboring cell. Agrawal discloses in paragraph **0029, lines 20-28** in the mobile station

receiving packets through the candidate IP subnetwork before a handoff is performed to a first of said at least one new IP subnetwork [as disclosed in **paragraph 0029, lines 20-28, upon the mobile sensing the presence of a neighboring base station's identity** (identity is achieved via a beacon-like packets from the candidate AP), **the mobile station will automatically relay the neighboring base station's identity through its serving base station to the address server, the address server (dynamically) then transmits the IP address of the neighboring base station to the mobile. This IP-layer authentication is need by the user (mobile) as mentioned in paragraph 0035 before the user (mobile) moves into the neighboring cell]**.

Regarding claim 3, Agrawal discloses in **fig. 2A** of a method for minimizing interruption in handoff of a mobile station **[mobile station 230, fig. 2A]** between access points in current **[access points 220-1n, fig. 2A]** and new subnetworks **[neighboring access points 220-1n, fig. 2A]**, comprising:

obtaining pre-authentication [obtaining layer 2 pre-authentication such as SIP or DNS and IP authentication information for the mobile station prior to the mobile station moving/disassociating with an access point in the serving cell to a neighboring cell, as disclosed in paragraphs 0035, 0041, and 0025 (lines 13-20)] for a mobile station [mobile station 233-1n, fig. 2A] that has a single wireless interface to work over an access point [each mobile station works wirelessly over an access point in the serving cell, see fig. 2A] in at least one new subnetwork [neighboring cell with neighboring access point 220-1n, fig. 2A] before dissociating [pre-authentication as mentioned above is obtained prior to moving/dissociating from serving

cell, see paragraph 0035] with an access point in the current subnetwork [current serving cell, access point 220-1n, fig. 2A] as claim.

Regarding claim 4, Agrawal discloses in **paragraph 0035** further including carrying said pre-authorization over an IP layer **[BS will send the mobile user necessary IP-layer authentication information before the user moves into the neighboring cell, see 0035].**

Regarding claim 6, Agrawal discloses a method, comprising:

resolving an IP address of an access point **[from the address server, paragraph 0029, lines 20-28]** in a new subnetwork when a mobile station is in a current subnetwork **[as disclosed in paragraph 0029, lines 20-28, upon the mobile sensing the presence of a neighboring base station's identity** (identity is achieved via a beacon-like message)**, the mobile station will relay the neighboring base station's identity through its serving base station to the address server, the address server then transmit (a probe response) resolving the IP address of the neighboring base station to the mobile when a mobile station is in a current serving subnetwork]**; and

obtaining pre-authentication for the mobile station to work over the current and new subnetworks using said IP address **[as disclosed in paragraph 0029, lines 2-9 and 20-28 in addition to paragraph 0035 (lines 1-8)**, upon the mobile device receiving the resolved IP address of the neighboring base station (access point), **a pre-authentication such as IP address for the mobile station is reserved/obtained from the neighboring cells prior to the user moving into the neighboring cell**. Note: IP Mobility ensures that the obtained new IP address

of the mobile device from the neighboring cells ensures communication with the neighboring base station (access point) from the current and the new subnetwork as long as there is signal].

Regarding claim 7, Agrawal disclose in **paragraph 0029, lines 20-28** wherein the resolving includes a dynamic resolution of the IP address [**upon the mobile sensing the presence of a neighboring base station's identity** (identity is achieved via a beacon-like message)**, the mobile station will automatically relay the neighboring base station's identity through its serving base station to the address server, the address server (dynamically) then transmits (a probe response) resolving the IP address of the neighboring base station to the mobile when a mobile station is in a current serving subnetwork**].

Regarding claim 8, Agrawal discloses in **paragraph 0029, lines 20-28**, wherein the dynamic resolution includes having an access point beacon ***(mobile station sensing the presence of a neighboring base station, Note a presence may only be sensed by a beacon/control/pilot packet)*** or probe response include an IP address **[as disclosed in paragraph 0029, lines 20-28, upon sensing a neighboring base station, mobile station receives a probe response from the address server with a dynamically resolved the IP address of the neighboring base station].**

Regarding claim 17, Agrawal discloses in **paragraph 0029** of communicating wherein said access point in the new subnetwork **[access point in the neighboring cell, fig. 2B]** supports higher-layer pre-authentication **[communicates MAC address to the mobile node and the**

mobile node is able to obtain higher level IP address of the node via address server, paragraph 0029] and communicates with the mobile station **[220, fig. 2B]** as claim.

Regarding claim 24, Agrawal discloses a method comprising:

reducing handoff delay **[reducing the time required for a mobiles station to obtain IP addresses needed for handoff, as in paragraph 0011]** of a mobile station **[mobile station 230, fig. 2A]** by

pre-establishing higher-layer contexts prior to handoff based on higher-layer pre-authentication **[pre-authenticating SIP or DNS as well as higher layer IP authentication information for the mobile station prior to the mobile station moving/disassociating with an access point in the serving cell to a neighboring cell, see paragraphs 0035-lines 1-8; 0041-lines 1-5, 7-22; and 0025-lines 13-20]**.

Regarding claim 25, Agrawal discloses **in paragraphs 0025, lines 13-20** wherein said higher-layer contexts include a client IP address in a new network **[the mobile station receives IP address for the new neighboring cell it will enter prior to enter a neighboring cell as in paragraph 0025, lines 13-20]** as claim.

Regarding claim 26, Agrawal discloses in **paragraph 0029, lines 20-28**, wherein said higher-layer contexts include a network address of the new network **[mobile station obtains the IP address of the neighboring base station (access point) as in paragraph 0029, lines 20-28]** as claim.

Regarding claim 55, Agrawal discloses in **fig. 2B** of a mobile communications network node **[mobile station 234-1n, fig. 2B]**, comprising:

a) a transceiver **[the mobile station 234-1n of fig. 2B receives and transmits data to access point 220, fig. 2B it serves]**;

b) Agrawal discloses means **[mobile station, fig. 2B]** for receives a network address from another mobile communications network node **[neighboring access point 220-1n, fig. 2B]** in a different network or subnetwork **[neighboring cell in on a different IP subnet, paragraph 0033]** for higher-layer pre-authentication **[IP address]** between said mobile communications network node **[mobile station, fig. 2B]** and said another mobile communications network node **[neighboring cell in on a different IP subnet, paragraph 0033]** while said nodes mobile are in the different networks or subnetworks.

[As disclosed in paragraph 0029, the mobile station 230 in one network is able receive and to obtain the pre-authentication IP address of the neighboring access point located in another subnet via a (probe response) resolved address server upon the mobile station sensing (Note: a beacon/pilot or control channel enables sensing) a neighboring base station's (access point) identity].

Regarding claim 56, Agrawal discloses in **fig. 2B**, wherein said mobile communications network node is a mobile node 230 as claim.

Regarding claim 57, Agrawal discloses in **fig. 2B** wherein said mobile communications network node is an access point or router 220-1n as claim.

Regarding claim 59, Agrawal discloses further including means **[mobile station 230, fig. 2B]** for establishing higher-layer contexts **[new client IP address (see paragraph 0025, lines 13-20 and paragraph 0024); new AP address (see paragraph 0029, lines 20-28); and DNS address (paragraph 0041, lines 1-5, 17-22)]** with said another mobile communications network node while **[access point 230]** said nodes are in the different networks or subnetworks **[as in paragraph 0033]** as claim.

3. Claims 44 and 46 rejected under 35 U.S.C. 102(b) as being anticipated by Vakil et al. (U.S. Pub. 2002/0167921), hereinafter referred as Vakil.

Regarding claim 44, Vakil discloses in **fig. 2** a method comprising:

performing a virtual soft handoff **[paragraph 0028 and fig. 2]** of a mobile device **[mobile station 201, fig. 2]** between access points **[access points 204c, fig. 2]**in proximate networks or subnetworks **[203c, fig. 2]** to minimize communication interruption **[0006, soft handoff ensures communication without/minimal interruption]** by allowing the mobile device to send and receive packets from a new one of said access points prior to handoff **[as disclosed in paragraph 0027-0028 and fig. 2 of performing virtual soft hand-off by the mobile device 201obtaining the necessary**

radio parameters and IP address from DHCP process within a new subnet upon detecting a pilot packet 205c of BS/access point 204c in the new subnet 203c].

Regarding claim 46, Vakil discloses in **paragraph 0002 and 0020** further including of using a lower-layer such as a physical CDMA transmission technology environment for providing a virtual soft handoff in an end-to-end IP wireless communication system. **CDMA technology provides reduction in communication interruption by its code technology, see paragraph 0006-0007.**

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

5. Claims 38, 39, and 41-43 rejected under 35 U.S.C. 102(a) as being anticipated by Hsieh et al ("A Comparison of Mechanisms for Improving Mobile IP Handoff Latency for End-to-End TCP").

Regarding claim 38, Hsieh et al. discloses on **page 2, section 2.2, 2nd paragraph** of a method:

performing higher-layer pre-authentication **[pre-registration of Layer 3 IP address prior to handoff as disclosed on page 2, section 2.2-2nd paragraph]**, pre-configuration **[pre-registration on mobile prior to hand-off as disclosed on page 2, section 2.2-2nd paragraph]**

and data traffic redirection [handoff] to reduce or eliminate timing dependency of a higher-layer handoff on a lower-layer handoff of a mobile station between access **networks [as disclosed on page 2, section 2.2-2nd paragraph, the configuring (pre-registering) an address (layer 3, IP address) for the mobile node in a network that it is likely to move to, before it moves, provides a data traffic redirection (handoff) that provides reduced/low latency, which is not dependent on L2 triggers]** as claim.

Regarding claim 39, Hsieh et al discloses in the **abstract, lines 10-12 and on page 2, section 2.1, paragraph 1** wherein said higher-layer handoff is a mobile IP handoff as claim.

Regarding claim 41, Hsieh et al discloses on **page 2, section 2.1, paragraph 1** of a mobile IP handoff. IP according to the OSI model is transmitted at the network layer, which is the 3rd layer of the OSI model clearly establishing that the higher-layer handoff (3rd layer IP handoff) includes an OSI network layer handoff.

Regarding claim 42, Hsieh et al discloses on **page 2, section 2.2, 2nd paragraph, lines 5-7** of further including initiating the higher-layer handoff earlier than the lower-layer handoff as claim.

Regarding claim 43, Hsieh et al discloses on **page 2, section 2.2, 2nd paragraph, lines 5-7** of further including completing the higher layer handoff entirely before the lower layer handoff as claim.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claim 9 rejected under 35 U.S.C. 103(a) as being unpatentable over Agrawal (U.S. Pub. 2002/0118656) in view of Liebsch et al. (Candidate Access Router Discover" ...see IDS).

Regarding claim 9, *Agrawal fails to disclose of using a CARD mechanism for a dynamic resolution.* Liebsch et al. Discloses in section 3.1, where a mobile node listen to L2 ID of new access points prior to making a decision about IP-level handover to Candidate Access Router (CAR), the candidate access routing protocol (CARD enable the MN to map the received L2 ID of an AP to the IP address of the associated CAR that connects to the AP. Liebsch further discloses in section 4, 1st paragraph that CARD protocol enable mobile node to perform dynamic resolution by enabling mobile nodes to handover to the resolved IP address of the associated CAR.

Therefore, it would have been obvious to one of ordinary skills in the art at the time of the invention to modify the teachings of Agrawal to include a utilizing the CARD protocol as taught by Liebsch. One is motivated as such in order to resolve the IP address of the candidate access router (base station) to enable seamless IP-layer handover of a mobile node from one access router to another *(Liebsch et al, Abstract).*

8. Claims 10 and 11 rejected under 35 U.S.C. 103(a) as being unpatentable over Agrawal (U.S. Pub. 2002/0118656) in view of Dorms ("Dynamic Host Configuration Protocol," RFC 2131, March 1997).

Regarding claim 10, Agrawal discloses in paragraph 0029, lines 20-28 of address resolution being performed by an address server. *Agrawal explicitly fails to disclose wherein said resolving includes a static resolution of the IP address.* Dorms discloses in on page 14, 2nd paragraph, where a DHCP carries a list pair of Hardware address (MAC) and IP address for the new network. In addition, according to the specification on page 25 of the current application, Dorms teaches that the DHCP carries a list of pairs of MAC and IP address for each nearby AP and such DHCP is being used in Dorms reference is categorized as a static resolution. Therefore, it would have been obvious to one of ordinary skills in the art at the time of the invention to modify the teachings of Agrawal to include the features of resolving the new network IP address by a static resolution using DHCP. One is motivated as such in order to resolve and allocate a network address to a client that will be connected from one network to another for communications.

Regarding claim 11, Agrawal discloses in paragraph 0029, lines 20-28 of address resolution being performed by an address server. *Agrawal explicitly fails to disclose wherein said resolving includes a static resolution of the IP address and the static resolution includes using DHCP for carrying a list of pairs of the MAC addresses and IP addresses for at least one nearby AP.* Dorms discloses in on page 14, 2nd paragraph, where a DHCP carries a list pair of Hardware address (MAC) and IP address for the new network. In addition, according to the

specification on page 25 of the current application, Dorms teaches that the DHCP carries a list of pairs of MAC and IP address for each nearby AP and such DHCP is being used in Dorms reference is categorized as a static resolution. Therefore, it would have been obvious to one of ordinary skills in the art at the time of the invention to modify the teachings of Agrawal to include the features of resolving the new network IP address by a static resolution using DHCP. One is motivated as such in order to resolve and allocate a network address to a client that will be connected from one network to another for communications.

9. Claim 12 rejected under 35 U.S.C. 103(a) as being unpatentable over Agrawal (U.S. Pub. 2002/0118656) in view of Palekar et al ("Protected EAP Protocol (PEAP) Version 2," 26 October 2003).

Regarding claim 12, Agrawal discloses in paragraph 0029, lines 20-28 of address resolution being performed by an address server. *Agrawal fails to disclose wherein said static resolution includes using EAP-TLV for carrying a list of pairs of the MAC addresses and IP addresses for at least one nearby access point.* Palekar et al discloses in section 4.7 that EAP-TLV contain 802.11 MAC address and SSID and further discloses on page 37 that EAP-TLV contain information on the identity of the peer and authenticator (layer 2 or IP addresses). In addition, according to the specification on page 25 of the current application, Palekar et al reference uses PEAP and the list may need to be sent from the tunneling end-point in a backend authentication server to achieve the desired resolution. Therefore, it would have been obvious to one of ordinary skills in the art at the time of the invention to modify the teachings of Agrawal to include the features of resolving using EAP-TLV. One is motivated as such in order to resolve

and allocate a network address to a client that will be connected from one network to another for communications.

10. Claims 5, 18, 28-30 and 58 rejected under 35 U.S.C. 103(a) as being unpatentable over Agrawal (U.S. Pub. 2002/0118656) in view of Aboba ("IEEE 802.1x Pre-Authentication"-July 17, 2002).

Regarding claim 5, Agrawal discloses in paragraph 0029 that access point in the neighboring cell communicates with a remote mobile station prior to handoff. *Agrawal fails to explicitly disclose further including carrying 802.1X over IP.* Aboba discloses on page 24, 4th paragraph that IEEE 802.1x pre-authentication functionality can be subsequently extended such as via support for AP advertisement over IP or EAP authentication over IP. Therefore, it would have been obvious to one of ordinary skills in the art at the time of the invention to modify the teachings of Agrawal to include the features pre-authentication 802.1x over IP as taught by Aboba. One is motivated as such in order to enable secure and low latency roaming *(Aboba, page 3).*

Regarding claim 18, Agrawal discloses in paragraph 0029 that access point in the neighboring cell communicates with a remote mobile station prior to handoff. ***Agrawal** fails to disclose wherein the communication with the mobile remote station is by using a higher-layer protocol that carries 802.1X frames.* Aboba discloses on page 5, 4th bullet, it is possible for STAs (Access Points) to authenticate prior to association according to IEEE 802.1x and further discloses on page 5, last paragraph that IEEE 802.1x per-authentication permits a STA to

authenticate to multiple STA while associating to only one STA. Therefore, it would have been obvious to one of ordinary skills in the art at the time of the invention to modify the teachings of Agrawal to include the features of AP from new subnetwork to communicate with remote mobile station using 802.1x frames. One is motivated as such in order to enable secure and low latency roaming (Aboba, page 3).

Regarding claim 28, Agrawal discloses in paragraph 0029 that access point in the neighboring cell communicates with a remote mobile station prior to handoff. *Agrawal fails to disclose of further including securing messages used for pre-establishing higher-layer contexts.* Aboda discloses on page 21-4th paragraph to page 22-1st and 4th paragraphs of further including securing messages [EAPOL-key message is exchanged, page 21-4th paragraph to page 22-1st paragraph] used for pre-establishing higher-layer contexts. Therefore, it would have been obvious to one of ordinary skills in the art at the time of the invention to modify the teachings of Agrawal to include transferring securing messages as taught by Aboda. One is motivated as such in order to enable secure and low latency roaming *(Aboda, page 3).*

Regarding claim 29, Agrawal discloses in paragraph 0029 that access point in the neighboring cell communicates with a remote mobile station prior to handoff. *Agrawal fails discloses further including using a higher-layer authentication protocol for deriving cipher keys for protecting higher-layer pre-configuration messages.* Aboda discloses on pages 25, lines 17-37 of utilizing an EAP-extended authentication protocol for deriving PTK (Pairwise Transient Key) and GTK (Group Transient Key) for protecting pre-configuration messages. Therefore, it

would have been obvious to one of ordinary skills in the art at the time of the invention to modify the teachings of Agrawal to include utilizing EAP for deriving exchange keys as taught by Aboda. One is motivated as such in order to enable secure derivation of key assuring authentication for low latency roaming *(Aboba, pages 3 and 25).*

Regarding claim 30, Agrawal discloses in paragraph 0029 that access point in the neighboring cell communicates with a remote mobile station prior to handoff. *Agrawal fails to disclose further including performing layer-2 pre-configuration by using 802.1X pre-authentication and 802.1X over IP.* Aboba discloses on page 5, 4th bullet, it is possible for STAs (Access Points) to authenticate prior to association according to IEEE 802.1x and further discloses on page 5, last paragraph that IEEE 802.1x per-authentication permits a STA to authenticate to multiple STA while associating to only one STA. Aboda discloses on page 24, 4th paragraph that IEEE 802.1x pre-authentication functionality can be subsequently extended such as via support for AP advertisement over IP or EAP authentication over IP. Therefore, it would have been obvious to one of ordinary skills in the art at the time of the invention to modify the teachings of Agrawal to include the features of performing layer 2 pre-authentication by using 802.1x pre-authentication and 802.1x over IP as taught by Aboba. One is motivated as such in order to enable a secure and low latency roaming *(Aboba, page 3).*

Regarding claim 58, Agrawal discloses in paragraph 0029 that access point in the neighboring cell communicates with a remote mobile station. *Agrawal fails to explicitly disclose further including means for storing higher-layer contexts for a security association with said*

another mobile communications network node while said nodes are in the different networks or subnetworks. Aboba discloses in section 4.1 on page 22 paragraph 1 that mobile station pre-authenticates by storing authentication and key management information of the other stations that it is likely to roam to. Aboba furthermore discloses on page 24, paragraph 4 that IEEE 802.1x pre-authentication supports AP advertisement over IP (higher layer). Therefore, it would have been obvious to one of ordinary skills in the art at the time of the invention to modify the teachings of Agrawal to include the feature of storing in the mobile unit security associations of another mobile communications node as taught by Aboba. One is motivated as such in order to support fast, secure low latency roaming (Aboba, pg 3).

11. Claims 19 and 20, rejected under 35 U.S.C. 103(a) as being unpatentable over Agrawal in view of Aboda as applied to claim 18 above, and further in view of Forsberg et al ("Protocol for Carrying Authentication for Network Access," October 23, 2003).

Regarding claim 19, Aboda et al discloses on page 5 (bullet 4) to improve scalability EAP messages must be used with 802.1x frames. Agrawal in view of Aboda et al fail to disclose further of maintaining order invariance of EAP messages. Forsberg et al disclose on page 1 of Protocol for carrying authentication for network access (PANA). Forsberg et al further discloses on pages 22, 23 and 45 that PANA carries EAP message to provide a session key in order to establish authentication. In addition, according to the specification on page 25 of the current application, since PANA is designed to carry EAP messages by nature, it has a mechanism to maintain order invariant. Therefore, it would have been obvious to one of ordinary skills in the art to modify the teachings of Agrawal in view of Aboda et al to include the feature of PANA

that maintains order of invariance as taught by Forsberg et al. One is motivated as such in order to provide an overall secure network access service including mechanisms for service provisioning, access control, authentication and accounting.

Regarding claim 20, Aboda et al discloses on page 5 (bullet 4) to improve scalability EAP messages must be used with 802.1x frames. Agrawal in view of Aboda et al fail to disclose further including using PANA for carrying EAP messages. Forsberg et al disclose on page 1 of Protocol for carrying authentication for network access (PANA). Forsberg et al further discloses on pages 22, 23 and 45 that PANA carries EAP message to provide a session key in order to establish authentication. In addition, according to the specification on page 25 of the current application, since PANA is designed to carry EAP messages by nature, it has a mechanism to maintain order invariant. Therefore, it would have been obvious to one of ordinary skills in the art to modify the teachings of Agrawal in view of Aboda to include the feature of PANA as taught by Forsberg et al. One is motivated as such in order to provide overall secure network access service including mechanisms for service provisioning, access control, authentication and accounting.

12. Claim 21 rejected under 35 U.S.C. 103(a) as being unpatentable over Agrawal in view of Aboda as applied to claim 18 above, and further in view of Nyberg (U.S. Patent No. 2005/0076216)

Regarding claim 21, Agrawal in view of Aboda fail to disclose further including using IKEv2 for carrying EAP messages. Nyberg teaches a method for securing a communication.

Nyberg discloses in paragraph 0032 and in claim 24 of a pre-authentication wherein the EAP messages use IKEv2, where the EAP messages may be authenticated using the second key. Therefore, it would have been obvious to one of ordinary skills in the art at the time of the invention to modify the teachings of Agrawal in view of Palekar et al to include the feature of using IKEv2 for carrying EAP messages as taught by Nyberg. One is motivated as such in order to establish a strong encryption and pre-authentication of the messages to be sent (Nyberg, paragraph 00150).

13. Claims 27 rejected under 35 U.S.C. 103(a) as being unpatentable over Agrawal in view of Rezaiifar (US 2004/0085931).

Regarding claim 27, Agrawal discloses in paragraph 0029, lines 20-28 of the mobile station obtaining IP address of the neighboring node prior to handoff. *Agrawal fails to explicitly disclose wherein said higher-layer contexts include a subnet mask of the new network.* Rezaiifar discloses in fig. 3 and paragraph 0054 that when a MS 2 leaves the coverage area 8 with respect to RANb, the MS 2 decodes the new subnet mask broadcasted by the neighboring RANc. The subnet mask for RANb and RANc are different because they are both on different networks. The address of the new subnet of RANc allows MS 2 to establish a session onto the neighboring network. Therefore, it would have been obvious to one of ordinary skills in the art at the time of the invention to modify the teachings of Agrawal to include a subnet mask with the network address prior to handoff as taught by Rezaiifar. One is motivated as such in order to perform seamless handoff of a mobile station between radio access networks having different wireless interfaces during wireless packet data service operation *(Rezaiifar, paragraph 0002).*

14. Claims 35 rejected under 35 U.S.C. 103(a) as being unpatentable over Agrawal in view of Adrangi et al. (US Pub. 2004/0120328), hereinafter referred as Adrangi.

Regarding claim 35, Agrawal discloses in fig. 2A of a method for performing a handoff of a mobile station **[mobile station 230, fig. 2A]** between access points **[current and neighboring access points 220-1n, fig. 2A]** in different access networks **[neighboring cells, fig. 2A and also see 0029 (lines 15-20) & 0032-where a new cell is served by different subnet]** with minimal interruption, comprising:

pre-establishing higher-layer contexts for the mobile station prior to handoff **[Agrawal discloses pre-authenticating SIP or DNS as well as higher layer IP authentication information for the mobile station prior to the mobile station moving/disassociating with an access point in the serving cell to a neighboring cell, as disclosed in paragraphs 0035 (Lines 1-8), 0041 (Lines 1-5, 7-22), and 0025 (lines 13-20)]**.

Agrawal discloses in paragraph 0041 that a Session Initiation protocol (SIP) and IP-layer registration and authentication may need to be preformed prior to roaming using the newly assigned address for communication. *Agrawal, however fails to explicitly disclose securely redirecting traffic originate from or destined for a pre-established IP address to a new access network.* Adrangi discloses in paragraph 0023-0024 that MN 140 may roam from subnet within Corporate Internet 100 to a subnet on External network 205. The MN must first registers with

the HAx (agent 305) and obtains its home address (pre-established IP address) and its care-of address on External Network, which may be obtained via DHCP server. MN 140 then establishes an IPSec Tunnel in order to redirect traffic. Therefore, it would have been obvious to one of ordinary skills in the art at the time of the invention to modify the teachings of Agrawal to include establishing a secure tunnel upon establishing external address as taught by Adrangi in order to provide a fast, seamless and secure roaming solutions across enterprise subnet *(Adrangi paragraphs 0001-00020)*.

15. Claims 40 rejected under 35 U.S.C. 103(a) as being unpatentable over Hsieh et al ("A Comparison of Mechanisms for Improving Mobile IP Handoff Latency for End-to-End TCP") in view of Adrangi et al. (US 2005/0113109), hereinafter referred as Adrangi.

Hsieh et al disclose on page 1 of higher layer handoff being a mobile IP handoff reducing latency. *Hsieh fails to disclose the higher-layer handoff is a VPN handoff.* Adrangi discloses in fig. 2, paragraphs 0013-0014 of a presence of a higher layer IPSec-based VPN when a mobile node attempts to roam between corporate intranet and an external network. IPSec-based VPN is used for handoff by establishing an IPsec tunnel to enable roaming with a corporate Internet from an external network. Therefore, it would have been obvious to one of ordinary skills in the art at the time of the invention to modify the teachings of Hsieh et al to include the feature of VPN handoff as taught by Adrangi. One is motivated as such in order to facilitate fast and secure mobile roaming *(Adrangi, paragraphs 0002-0003)*.

16. Claims 45 rejected under 35 U.S.C. 103(a) as being unpatentable over Vakil et al. (U.S. Pub. 2002/0167921), hereinafter referred as Vakil in view of Hsieh et al ("A Comparison of Mechanisms for Improving Mobile IP Handoff Latency for End-to-End TCP").

Regarding claims 45, Vakil disclose in fig. 2 of a virtual soft handoff between a mobile station and a base station. *Vakil fails to disclose of performing a higher layer handoff entirely before a lower layer handoff.* Hsieh et al teaches of low latency handoff. Hsieh et al discloses on page 2, section 2.2, 2nd paragraph, lines 5-7 of further including completing the higher layer handoff entirely before the lower layer handoff as claim. Therefore, it would have been obvious to one of ordinary skills in the art at the time of the invention to modify the teachings of Vakil to include the feature of completing the higher layer handoff entirely before the lower layer handoff as taught by Hsieh et al. One is motivated as such in order to perform a fast-handover to a new attachment point *(Hsieh, page 3, paragraph 1).*

17. Claims 52-54 rejected under 35 U.S.C. 103(a) as being unpatentable over Vakil et al. (U.S. Pub. 2002/0167921), hereinafter referred as Vakil in view of Apostolopoulos et al. (U.S. Pub. 2003/0009576), hereinafter referred as Apostolopoulous.

Regarding claim 52, Vakil disclose in fig. 2 of a virtual soft handoff between a mobile station and a base station. *Vakil fails to explicitly disclose that the mobile device may be a mobile telephone.* Apostolopoulous discloses in fig. 1 of performing a soft-handoff in a mobile streaming media system, having multiple base stations and a mobile client 902. Apostolopoulous further discloses in paragraph 0033 that the mobile client may be a cell phone, PDA, laptop computer, pager or the like. Therefore, it would have been obvious to one of

ordinary skills in the art at the time of the invention to modify the teachings of Vakil to include the teachings of the mobile station being a PDA, laptop computer or cell phone as taught by Apostolopoulous. One is motivated as such in order to provide diversification and span various types of client devices for performing non-real-time and real-time streaming communications.

Regarding claim 53, Vakil disclose in fig. 2 of a virtual soft handoff between a mobile station and a base station. *Vakil fails to explicitly disclose that the mobile device may be a mobile computer*. Apostolopoulous discloses in fig. 1 of performing a soft-handoff in a mobile streaming media system, having multiple base stations and a mobile client 902. Apostolopoulous further discloses in paragraph 0033 that the mobile client may be a cell phone, PDA, laptop computer, pager or the like. Therefore, it would have been obvious to one of ordinary skills in the art at the time of the invention to modify the teachings of Vakil to include the teachings of the mobile station being a PDA, laptop computer or cell phone as taught by Apostolopoulous. One is motivated as such in order to provide diversification and span various types of client devices for performing non-real-time and real-time streaming communications.

Regarding claim 54, Vakil disclose in fig. 2 of a virtual soft handoff between a mobile station and a base station. *Vakil fails to explicitly disclose that the mobile device may be a PDA*. Apostolopoulous discloses in fig. 1 of performing a soft-handoff in a mobile streaming media system, having multiple base stations and a mobile client 902. Apostolopoulous further discloses in paragraph 0033 that the mobile client may be a cell phone, PDA, laptop computer, pager or the like. Therefore, it would have been obvious to one of ordinary skills in the art at the time of

the invention to modify the teachings of Vakil to include the teachings of the mobile station being a PDA, laptop computer or cell phone as taught by Apostolopoulous. One is motivated as such in order to provide diversification and span various types of client devices for performing non-real-time and real-time streaming communications.

18. Claims 60 rejected under 35 U.S.C. 103(a) as being unpatentable over Agrawal in view of Vakil et al. (U.S. Pub. 2002/0167921), hereinafter referred as Vakil.

Regarding claim 60, Agrawal discloses in fig. 2A and in paragraph 0025 of a mobile station receiving a list of neighboring candidate cell IP addresses prior to the mobile station entering into a candidate/neighboring cell. *Agrawal fails to disclose the mobile communications node further including means for performing a virtual soft handoff between the different networks or subnetworks by allowing a mobile one of said nodes to send or receive traffic to the other of said nodes prior to handoff.*

Vakil discloses in **fig. 2**, a mobile node performing a virtual soft handoff **[paragraph 0028 and fig. 2]** of a mobile device **[mobile station 201, fig. 2]** between access points **[access points 204c, fig. 2]**in proximate networks or subnetworks **[203c, fig. 2]** to minimize communication interruption **[0006, soft handoff ensures communication without/minimal interruption]** by allowing the mobile device to send and receive packets from a new one of said access points prior to handoff **[as disclosed in paragraph 0027-0028 and fig. 2 of performing virtual soft hand-off by the mobile device 201obtaining the necessary radio parameters and IP address from DHCP**

process within a new subnet upon detecting a pilot packet 205c of BS/access point 204c in the new subnet 203c].

Therefore, it would have been obvious to one of ordinary skills in the art at the time of invention to include into Agrawal's invention a mobile node performing a virtual soft handoff prior to moving to a new subnet as taught by Vakil. One is motivated as such in order to provide more time for carrying out the hand-off procedure ensuring an increase in capacity and reliability (Vakil 0006).

Allowable Subject Matter

19. Claims 13-16, 22, 23, 31-34, 36, 37, and 47-51 objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Regarding claims 13-16, Prior Art fails to disclose wherein the access point in the new subnetwork does not support higher-layer pre-authentication and communicates with the mobile station via a proxy agent and the IP address is of the proxy agent in combination with other limitations set forth in the respective claim.

Regarding claim 22-23, Prior Art fails to disclose further including using a newly defined protocol to carry 802.1x frames over a reliable transport in combination with other limitations set forth in the respective claim.

Regarding claims 31-34, Prior Art fails to disclose further including using a single higher-layer authentication protocol for pre-establishing a plurality of the higher-layer contexts in combination with other limitations set forth in the respective claim.

Regarding claims 36-37, Prior Art fails to disclose further including establishing an Ipsec tunnel between the mobile station and an access router in the new access network, where an Ipsec tunnel inner address is bound to the pre-established IP address in combination with other limitations set forth in the respective claim.

Regarding claim 47, Prior Art fails to disclose further including controlling a layer-2 handoff timing by a higher layer so that pre-authentication and per-configuration can be completed prior to starting layer-2 handoff in combination with other limitations set forth in the respective claim.

Regarding claims 48-51, Prior Art fails to disclose further of including using an Ipsec tunnel for traffic redirection during a virtual soft-handoff, with outer and inner IP addresses of a device for the Ipsec tunnel being a care-of address in the current subnet and the care-of address in a new subnet, respectively in combination with other limitations set forth in the respective claim.

Conclusion

Any response to this action should be faxed to:

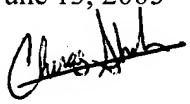
(571)272-8300, (for formal communications intended for entry)

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chirag G. Shah whose telephone number is 571-272-3144. The examiner can normally be reached on M-F 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Wellington Chin can be reached on 571-272-3134. The fax phone number for the organization where this application or proceeding is assigned is 571-272-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

cgs
June 13, 2005



Chrag Shah